CM.com

Cybersecurity @CM.com

Sándor Incze

Who am I

CISO

C|EH Certified Ethical Hacker

(ᵔᴥᵔ)

¯_(ツ)_/¯

- Formula 1
- Tickets
- Access Control
- Food and Beverage
- Realtime Messaging

[(5)]

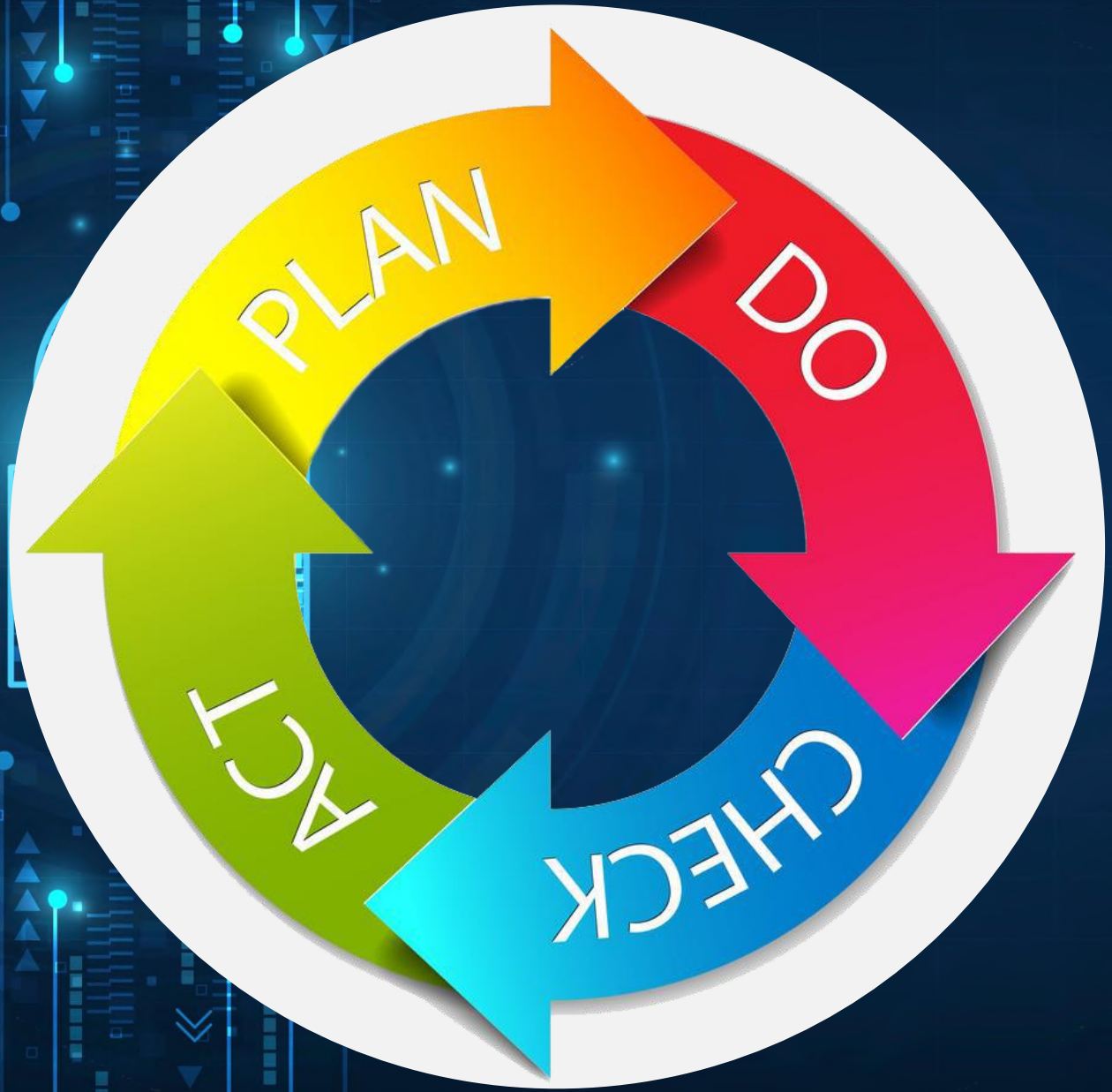
Police

Government

Financial Institutions

ᕕ(⌐ˆ_ˆ-")ᕗ

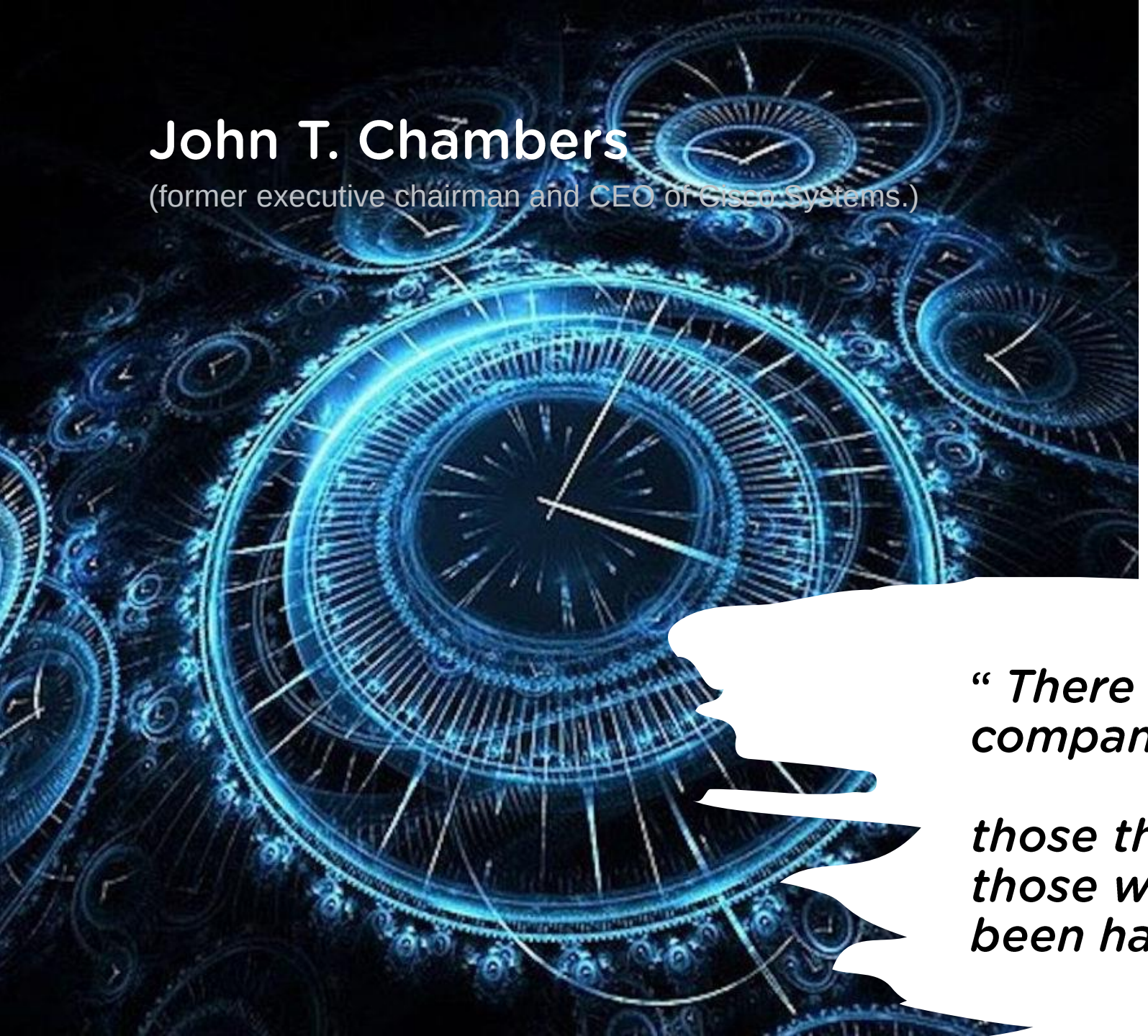
ISO27001 / 27017 & 27018



Cybersecurity @CM.Com

Robert MUELLER – FBI Director, 2012

“ There are only two types of companies: those that have been hacked, and those that will be. ”



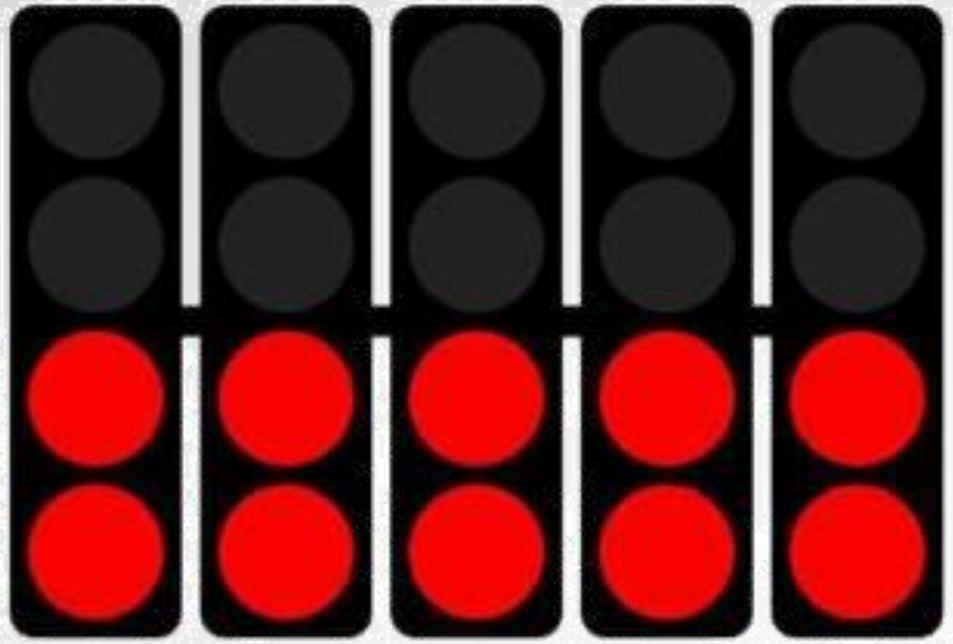
John T. Chambers

(former executive chairman and CEO of Cisco Systems.)

“ There are two types of companies:

those that have been hacked, and those who don’t know they have been hacked. ”


Businesses suffered
50% more cyber attacks
in 2022*
What do you see?

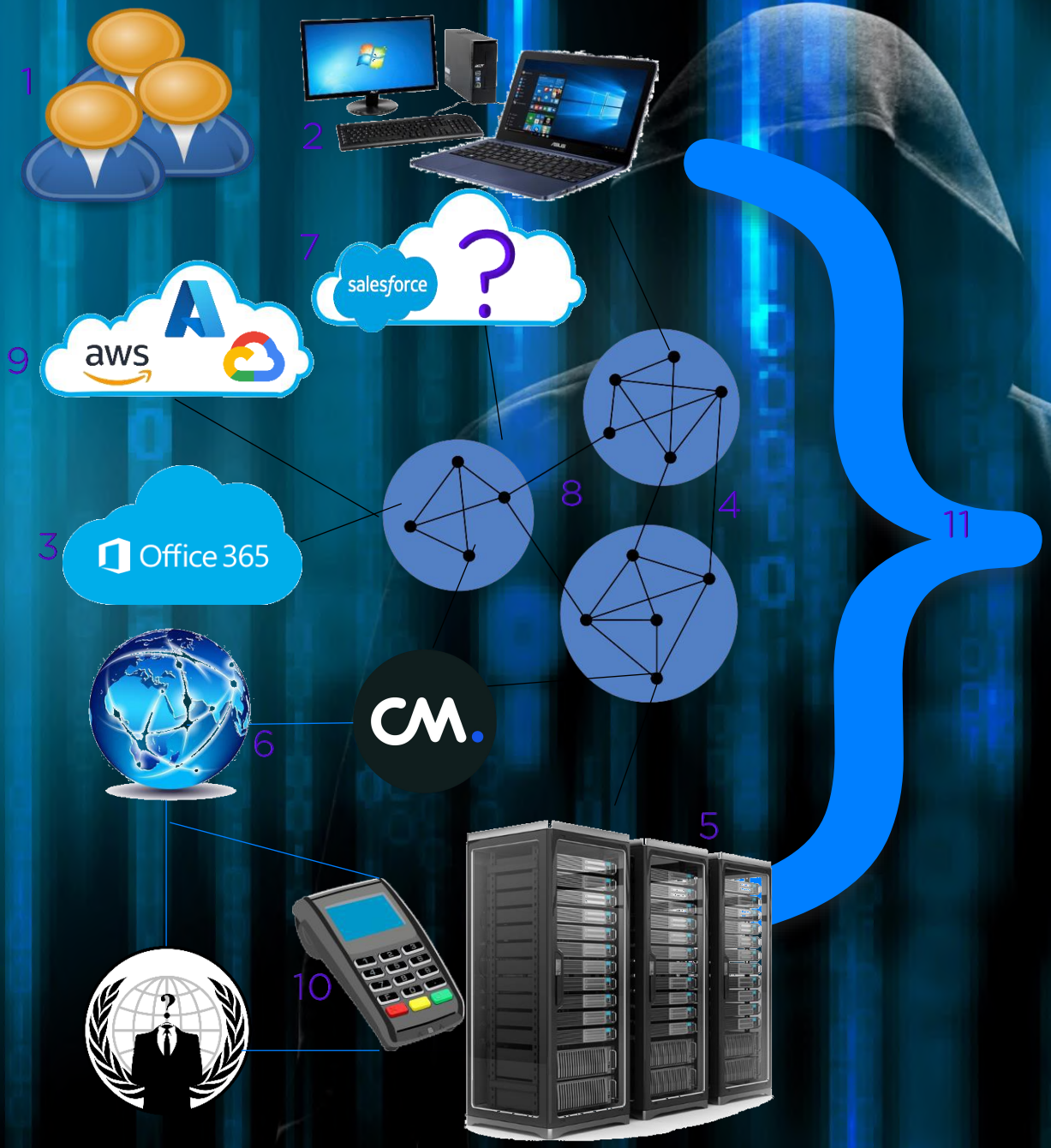


CM.

GET READY TO RACE!

HONDA
33
TAG HEUER
Red Bull
Mobil 1
ASTON MARTIN


TOP SECRET



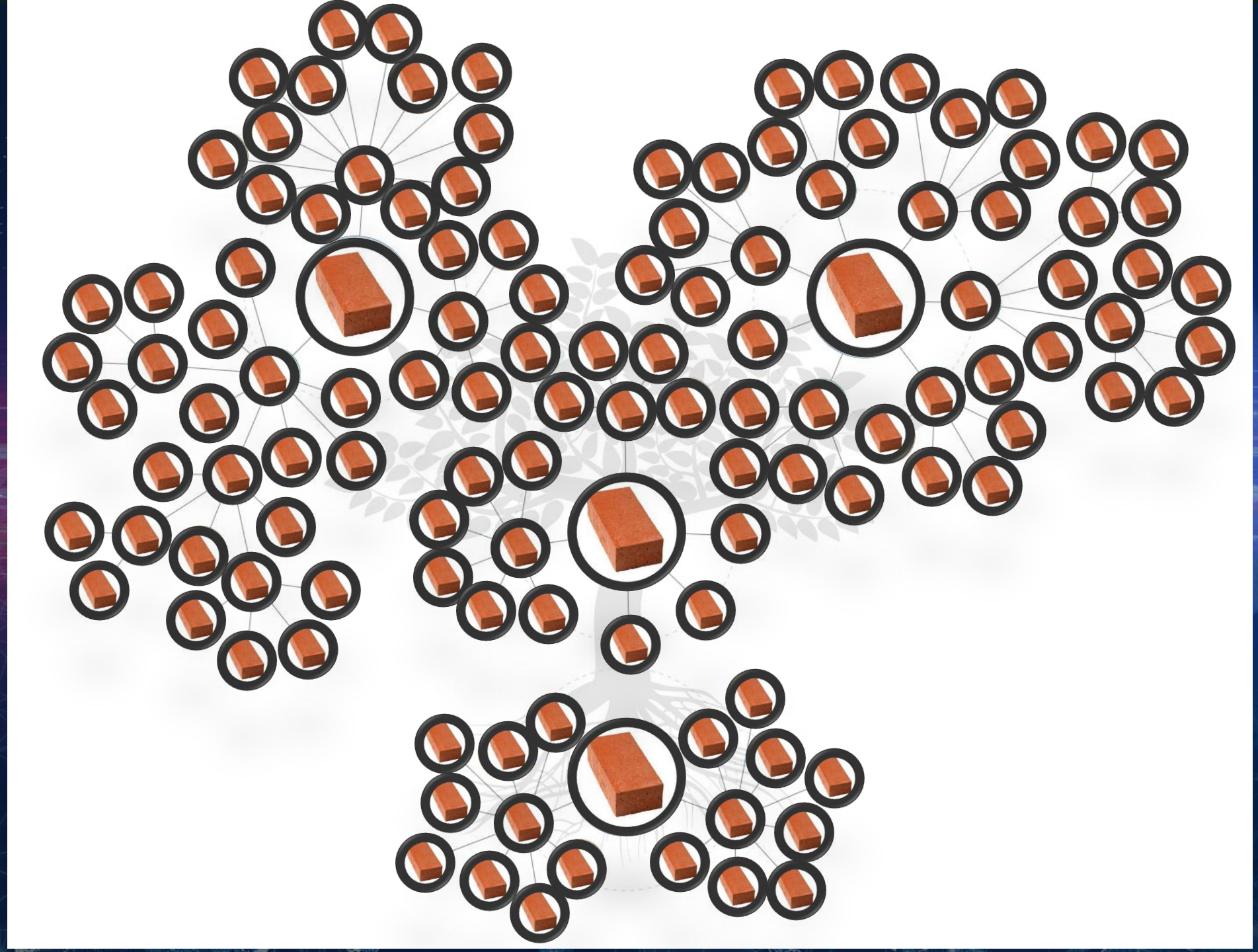
1. End-Users
   - Security Awareness Training
   - Secure Code training (dev)
   - *Password Manager*
2. Workstations
   - Endpoint Protection
   - OS + Patches (monitoring)
   - Applications + patch management
   - *Local user account Exploitation*
   - *Service account monitoring*
3. Email
   - Email Scanning (inbound) step 1 MS
   - Email Scanning (inbound) step 2 DT
   - Email Protection (outbound)
   - *Ofice macros Disabled*
4. Network
   - Network Scanning (traffic)
   - Network Segmentation (VLAN)
   - *Zero-Trust Access*
5. Servers
   - *Endpoint Protection*
   - OS + patch management
   - Applications + patch management
   - Vulnerability Scanning (Agents)
   - Penetration Testing (Q1, Q3)
   - Continuous Bug Bounty Program
   - Internal Penetration Testing
   - Back-up & Restore
   - *AD (Account Monitoring) Kerberos attack*
   - *No Direct Internet Access (log4J)*
   - *CF Workers*
6. Internet
   - WAF / DNS / CDN
   - Loadbalancer (3x)
   - SIEM
   - Modsec Rules
   - IDS / IPS
   - DDOS (Global on the edge)
   - Certificate Management
7. In Use (external) Cloud services
   - Acces ADFS / AD / SSO
8. (Cloud)Platform
   - DNS Change Management
   - SAST / DAST development
   - SDLC
   - Web Application Pentest Scanner
9. Cloud Service Providers
   - *Compliance Scanning*
   - *Monitoring*
10. POS Vulnerabilities

11. CM Security Team

Understand the basics.

CM Security Team

A few bricks to short!




cm.

SAST vs. DAST

The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks

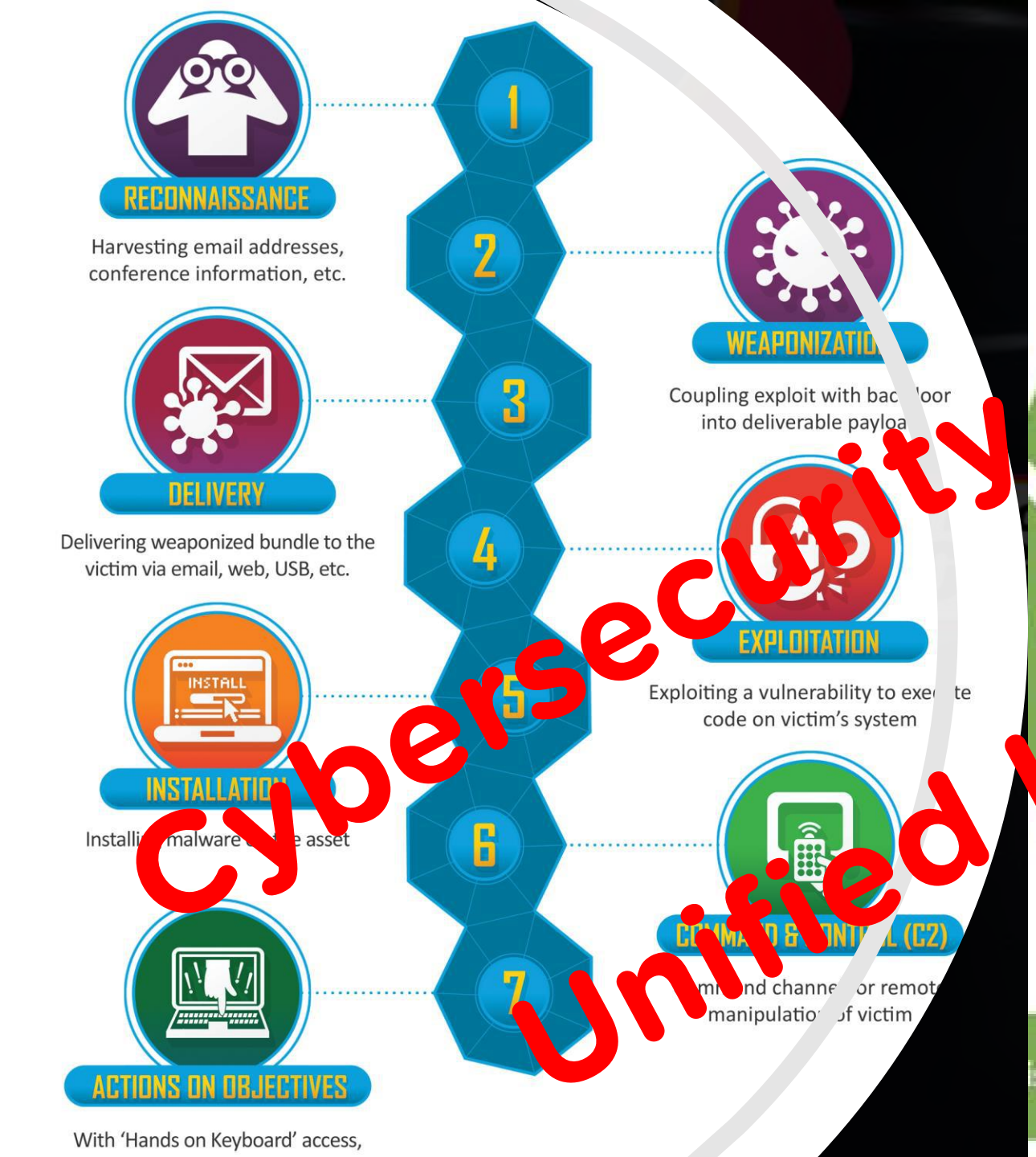
Enable multifactor authentication

Apply least privilege access

Keep up to date

Utilize antimalware

Protect data



Cybersecurity Kill Chain.

Unified Kill Chain


Reconnaissance
Mapping of Attack Surface
Initial Access
Initial Foothold within the network
Privilege Escalation
Obtained Highest Level Permission
Lateral Movement
Search for Sensitive Assets
Exfiltration
Data Theft

CM.COM CIRCUIT ZANDVOORT

Achieving the objective.

RECONNAISSANCE

STRATEGIC
Identify the *Who* and *Why*

OPERATIONAL
Address the *How* and *Where*

TACTICAL
Focus on the *What*

The Three Levels of Cyber Threat Intelligence.


STRATEGIC
Identify the Who and Why
Nation States
Corporate Spies
Criminal Groups
Malicious Insiders
Sources of Cybersecurity Threats
Hackers
Terrorist Groups
Hacktivists

Different hospitals in different countries targeted

Hospitals targeted by Russian cybercriminals Killnet . Including hospitals in the Netherlands, the United Kingdom, Spain, Finland, Norway, Poland and Germany. There are also attacks on hospitals in the USA. The DDoS campaign by Killnet started on January 28.

Мед учереждения Нидерланды :
http://www.umcutrecht.nl/ -- Университетский медицинский центр Утрехта
https://www.lumc.nl/ -- Университетский медицинский центр Лейда
http://www.radboudumc.nl/ -- Медицинский центр университета Радбуда
https://www.mumc.nl/ -- Медицинский центр Маастрихтского университета
https://www.erasmusmc.nl/en/ -- Медицинский центр Университета Эразмус
https://www.catharinaziekenhuis.nl/ -- Катарина Зикенхейс
https://www.jeroenboschziekenhuis.nl/ -- Больница Йеруна Боша
https://www.mmc.nl/ -- Медицинский центр Максима
https://www.mst.nl/ -- Medisch Spectrum Twente (MST)
https://reinierdegraaf.nl/
http://www.olvg.nl/ -- Onze Lieve Vrouwe Gasthuis (англ. "Больница Богоматери")
https://www.flevoziekenhuis.nl/
http://www.tjongerschans.nl/
https://www.nijsmellinghe.nl/
https://www.antonius-frl.nl/
https://www.mcl.nl/
https://www.umcg.nl/ -- Университетский медицинский центр Гронингена
https://www.treant.nl/
https://www.martiniziekenhuis.nl/
https://www.bernhoven.nl/
https://www.tweestedenziekenhuis.nl/

The Netherlands

Мед. Германии

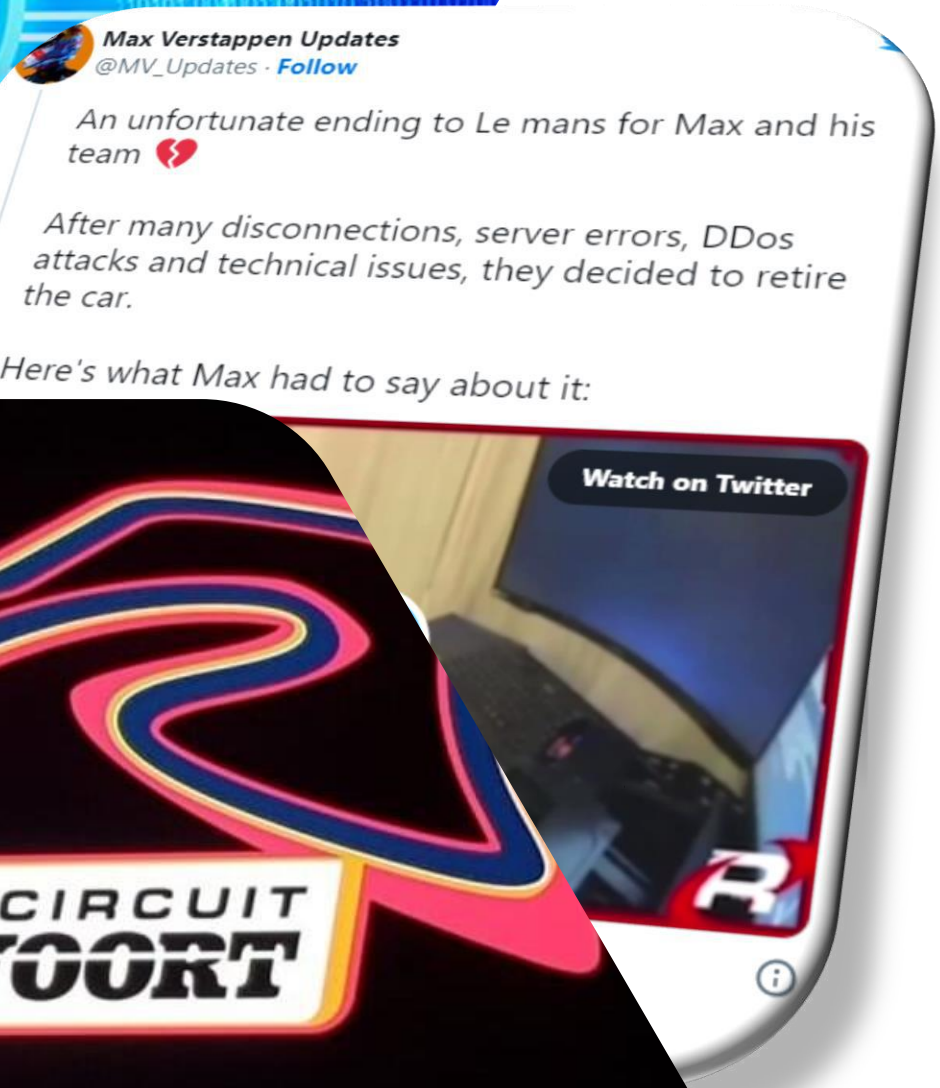
https://www.muenchen-klinik.de/
https://www.stadtkrankenhaus-schwabach.de
https://www.paracelsus-kliniken.de/
https://www.geomed-klinik.de/

мед учереждения Польши :
https://www.ukrainianinpoland.pl/ru/
https://polandlek.pl/
https://www.mp.pl/
https://vrachi.pl/

STRATEGIC
Identify the *Who* and *Why*

STRATEGIC
Identify the *Who* and *Why*

Publicly Listed Company.



- **STRATEGIC**
  Identify the *Who* and *Why*

Racing.

STRATEGIC
Identify the *Who* and *Why*

DDOS.

Sms認証通る日本の電話番号買えるサイトないですか?

2 **NO NAME** 2021-07-30 Fri 21:32:59

>>1
ないです
sms認証代工業者かフリマで売ってるSMS付きSIMを買ってください

CM.comのアングラ版で、アプリインストールして送受信一件毎にお小遣いくれるサービス
"Mobile SMS profit" "SMS Make Money" "Get paid for incoming SMS" で探せば出てくる
を態々英語で検索してインストールした馬鹿の電話番号が"SMS Receive Online"に稀に出てきますが、可能性は低いです。

3 **2** 2021-07-30 Fri 21:50:54

誰かが、SMS受信お小遣いアプリをインストールすると以下のサイトに載ります

https://sms-receive.net/buynumber.php
http://receive-sms-online.info/privatenumbers.php

4 **NO NAME** 2021-07-31 Sat 12:40:20

電話番号の音声認証で固定電話番号使えるサイト(Vプリカ等)なら
自前で電話鯖立てて、露助から日本の固定電話番号買って来れば
認証通ります

電話鯖から sip.tg へ転送し Tor経由でTelegram

Score: 41.74 | Language: English | Date Indexed: 29 Nov 2016, 12:30 UTC
Search for more hits within this domain. (2)

http://5b7lrclibipnhlrh6gubuvn5yojfmtchthvi2onxaqtc34vje53tldid.onion/black2/2pgq3b5r/l50
電話番号 | BLACK II ✔
Domain Page Cached (1) Page Source
2NO NAME2021-07-30 Fri 21:32:59 >>1 ないです sms認証代工業者かフリマで売ってるSMS付きSIMを買ってください **CM.com**のアングラ版で、アプリインストールして
Score: 22.67 | Language: English | Date Indexed: 02 Aug 2021, 01:31 UTC
Search for more hits within this domain. (3)

http://publicibkxahavzc.onion/websites/%22pub-4918407366062109%22/
"pub-4918407366062109" - 12 Websites - PublicWWW.com ✖
Domain Page Cached (1) Page Source
782 whatsmyserp.com gle_ad_client = "ca-pub-4918407366062109"; /* whatsmyserp to 59 213 inches-to-**cm.com**
Score: 21.59 | Language: English | Date Indexed: 06 May 2016, 15:02 UTC
Search for more hits within this domain. (1)

http://ca-es.facebookcorewwwi.onion/directory/pages/U
U | u n o f f i c i a l w o r m c o r e | Directori de pàgines ✖
Domain Page Cached (2) Page Source
krtl H chl ab Hawa aane De Usne kaha bhul jaao mujhe hmne kah diya kon ho tum - Uso carruzo la

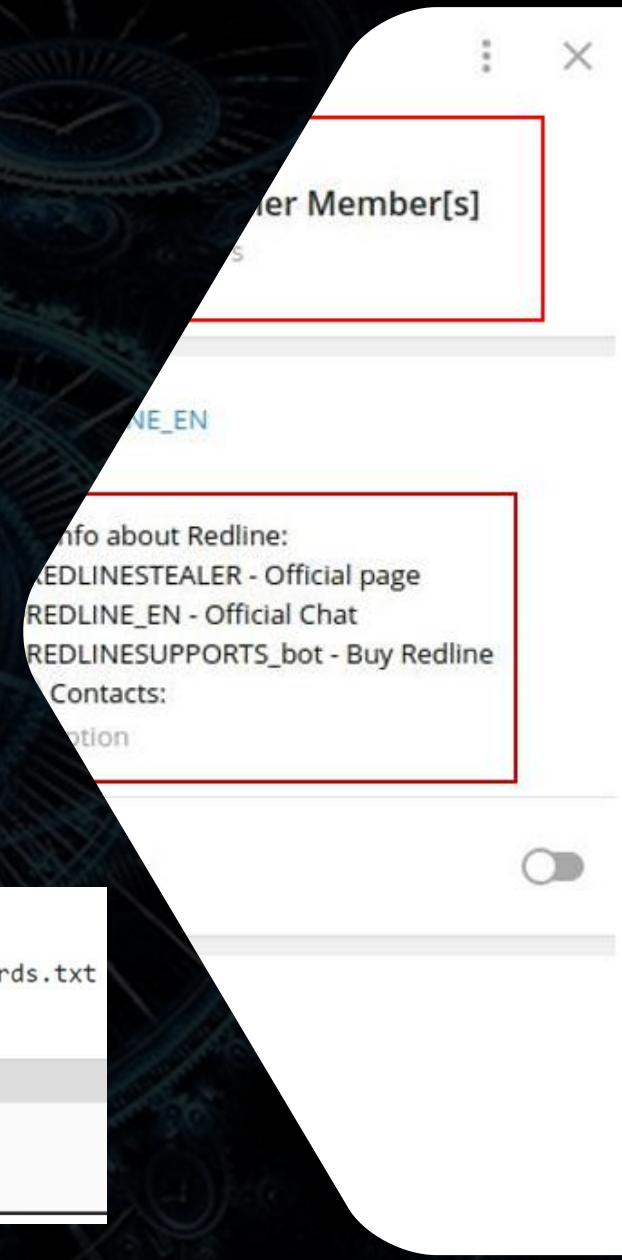
OPERATIONAL
Address the *How* and *Where*

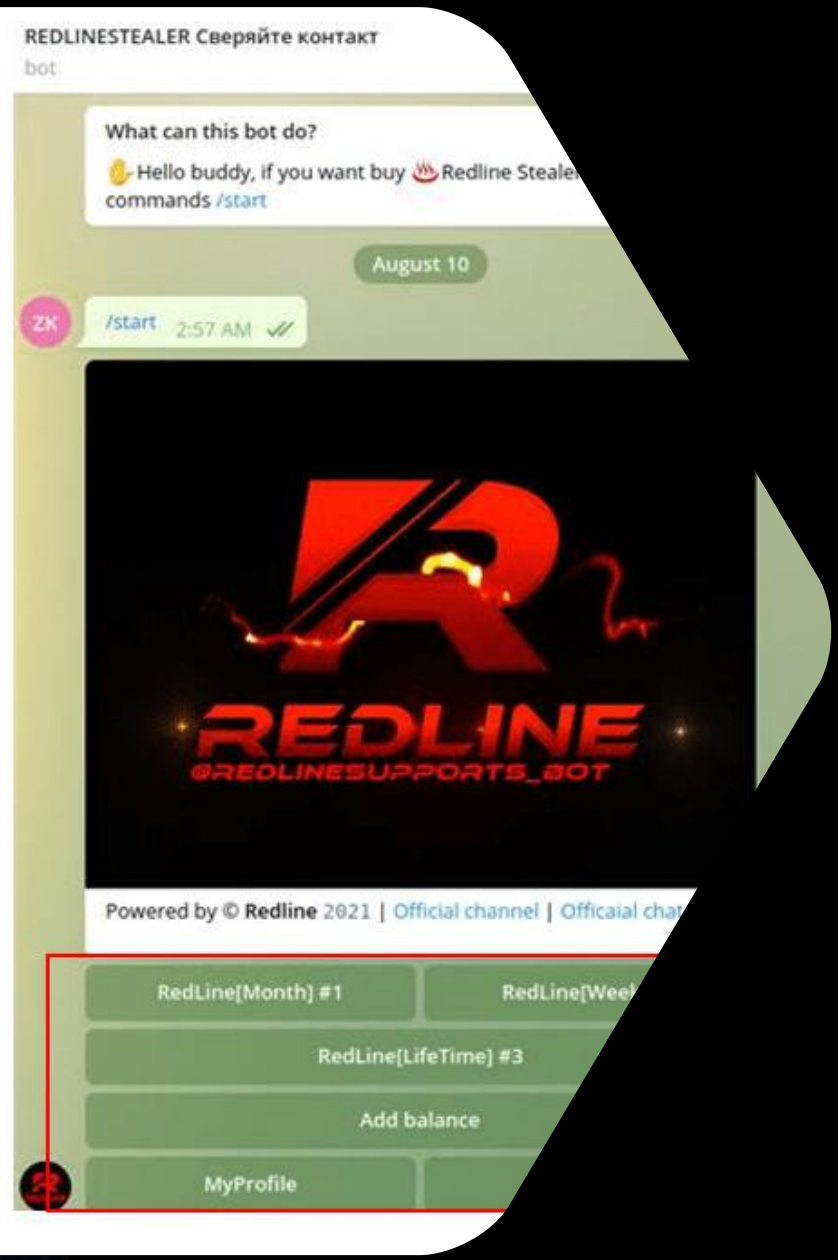
24x7 NOC

ᘓ(ò_ó˘)ᕑ

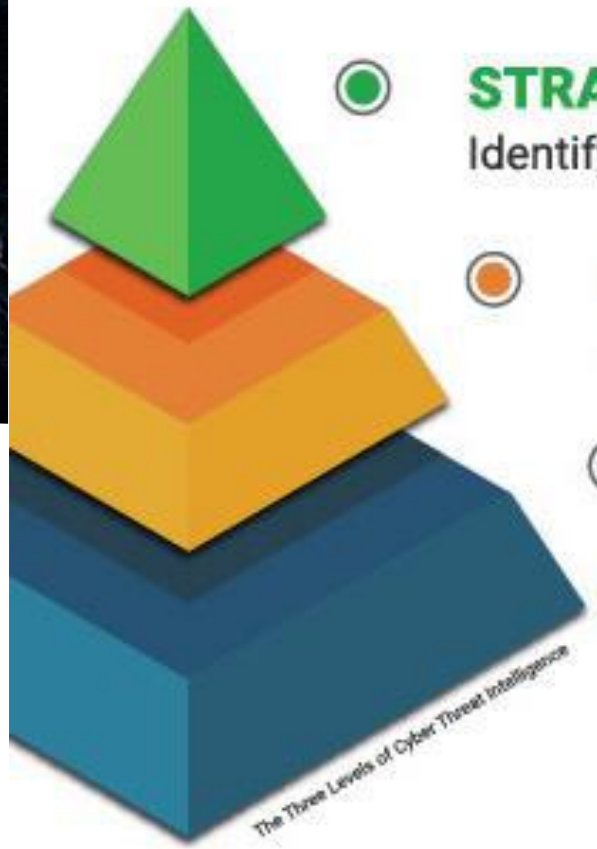
OPERATIONAL

Address the *How* and *Where*





ᘓ(ò_óˇ)ᘑ



STRATEGIC
Identify the *Who* and *Why*

OPERATIONAL
Address the *How* a

TACTICAL
Focus on the

Eternity Builder

Available products:

- 💳 Stealer (260$)
- 💸 Clipper (90$)
- 💳 Dropper (80$)
- ⛏ Miner (110$)
- 🕸 Worm (390$)
- 🔐 Ransomware (490$)

🔥 

TACTICAL
Focus on the *What*

How to Restore Your Files

Security Alert!!!

We hacked your company successfully

All files have been stolen and encrypted by us

If you want to restore files or avoid file leaks, please send **2.033763** bitcoins to the wallet [redacted]

If money is received, encryption key will be available on **TOX ID:** [redacted]

IOC

Attention!!!

Send money within 3 days, otherwise we will expose some data and raise the price

Don't try to decrypt important files, it may damage your files

Don't trust who can decrypt, they are liars, no one can decrypt without key file

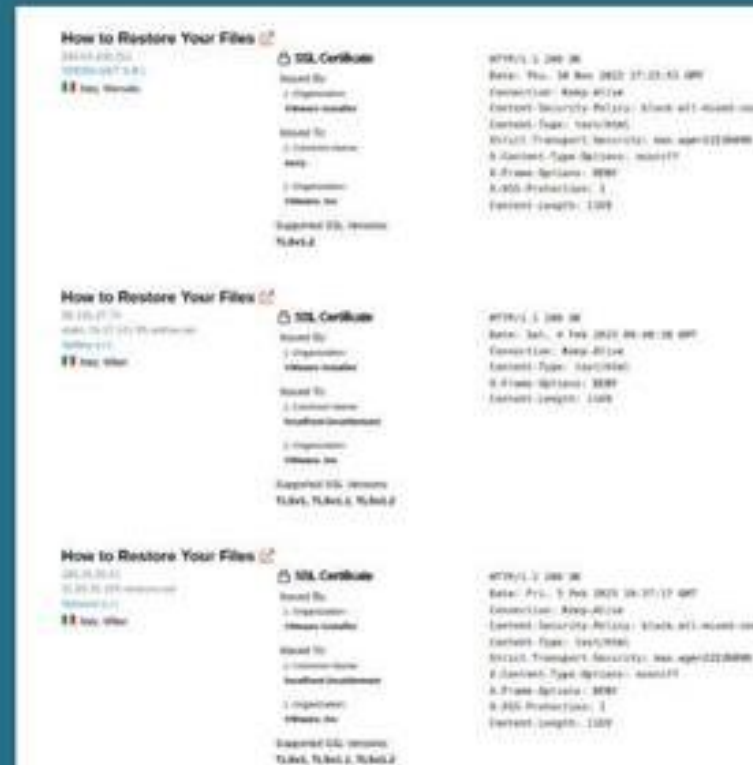
If you don't send bitcoins, we will notify your customers of the data breach by email and text message

And sell your data to your opponents or criminals, data may be made release

Note

SSH is turned on

Firewall is disabled



TACTICAL
Focus on the *What*

SHODAN | Explore | Downloads | Pricing | html:"TOX_ID" | Account

TOTAL RESULTS

382

TOP COUNTRIES

France	117
Germany	63
Canada	45
United States	43
United Kingdom	22

More...

TOP ORGANIZATIONS

OVH SAS	96
Hetzner Online GmbH	49
OVH Hosting, Inc.	43
OVH GmbH	14
OVH Ltd	8

More...

View Report | Download Results | Historical Trend | View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out Gravwell

How to Restore Your Files

2023-02-04T11:18:43.706373

212.32.251.106
s2114389.dedi.leaseweb.net
LeaseWeb Netherlands B.V.
Netherlands, Amsterdam

SSL Certificate
Issued By:
|- Organization:
VMware Installer
Issued To:
|- Common Name:
s2114389.dedi.leaseweb.net
|- Organization:
VMware, Inc
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Sat, 4 Feb 2023 11:18:43 GMT
Connection: Keep-Alive
Content-Type: text/html
X-Frame-Options: DENY
Content-Length: 1169
```

How to Restore Your Files

2023-02-04T11:11:06.301018

152.66.236.71
vmware2.vpk.bme.hu
Budapest University of Technology and Economics
Hungary, Budapest

SSL Certificate
Issued By:
|- Organization:
VMware Installer
Issued To:
|- Common Name:
vmware2.vpk.bme.hu
|- Organization:
VMware, Inc
Supported SSL Versions:
SSLv3, TLSv1, TLSv1.1, TLSv1.2

Vulnerabilities
Heartbleed

```
HTTP/1.1 200 OK
Date: Sat, 4 Feb 2023 11:11:06 GMT
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 1168
```

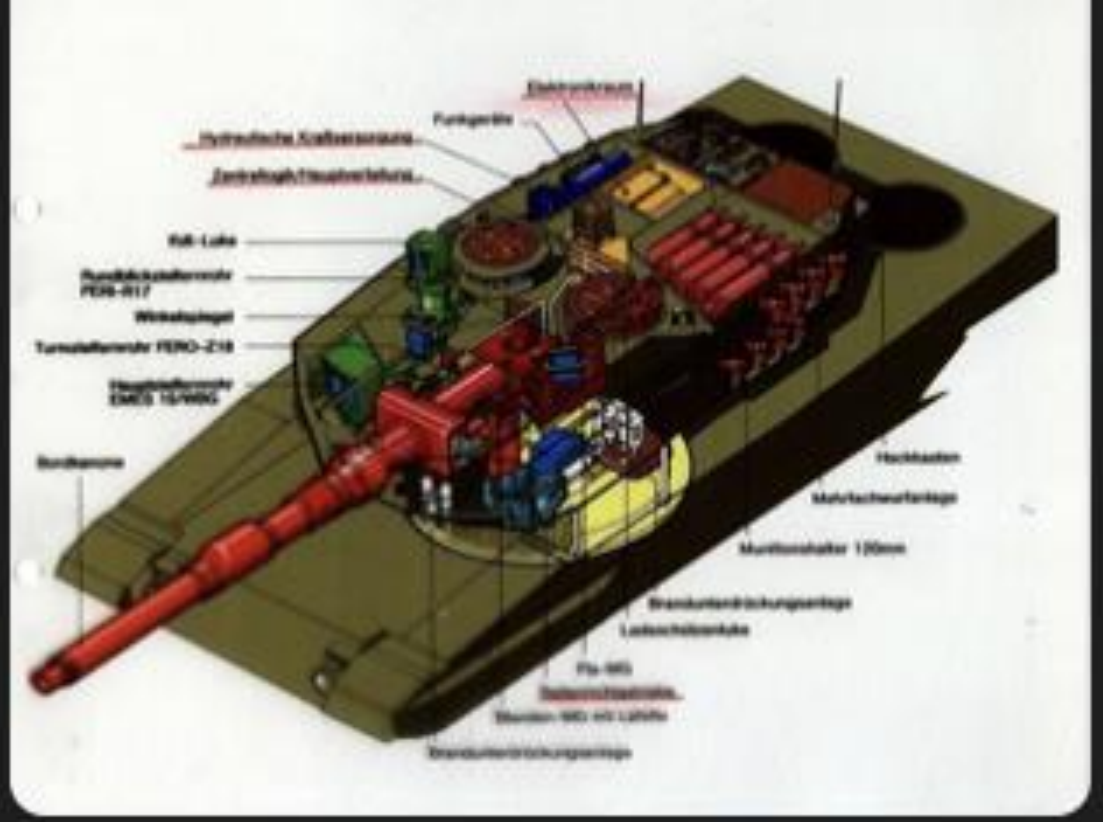
How to Restore Your Files

2023-02-04T11:09:47.325774

51.77.85.56
ns3144405.ip-51-77-8

SSL Certificate

```
HTTP/1.1 200 OK
```



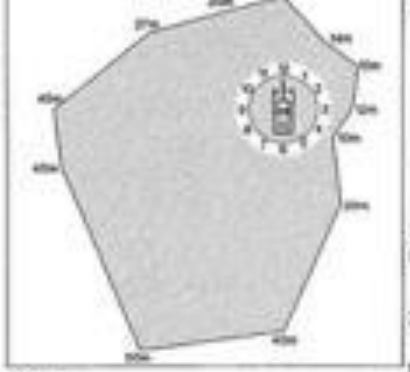


Bild 3

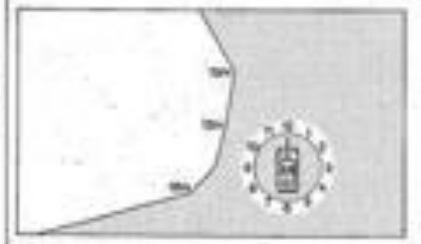
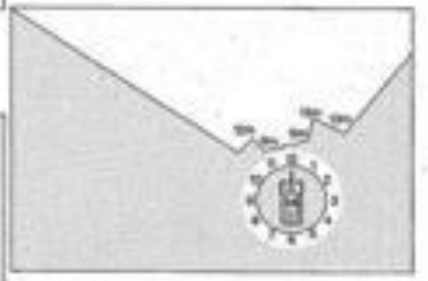


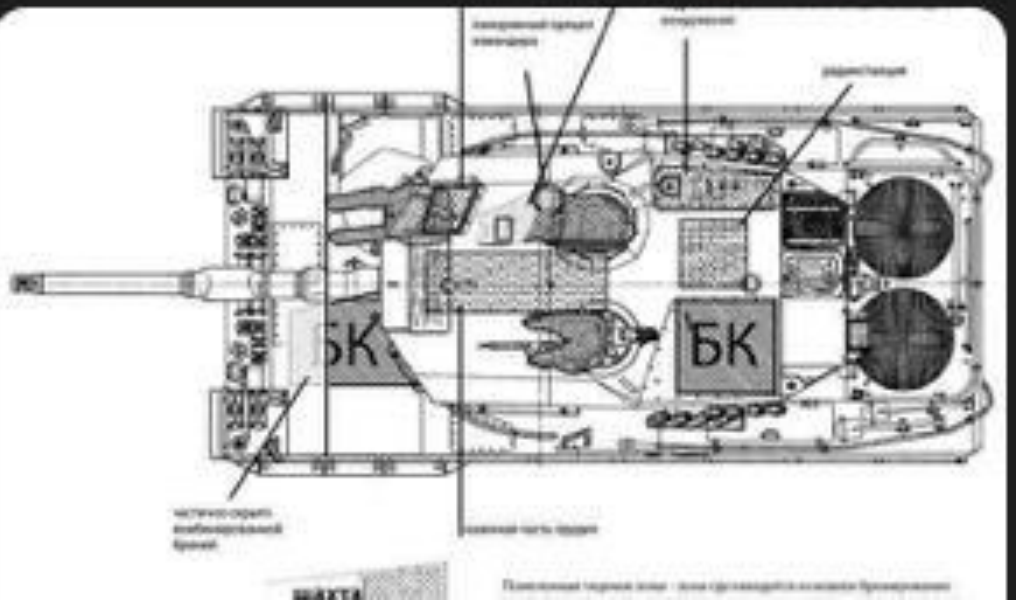
Bild 5

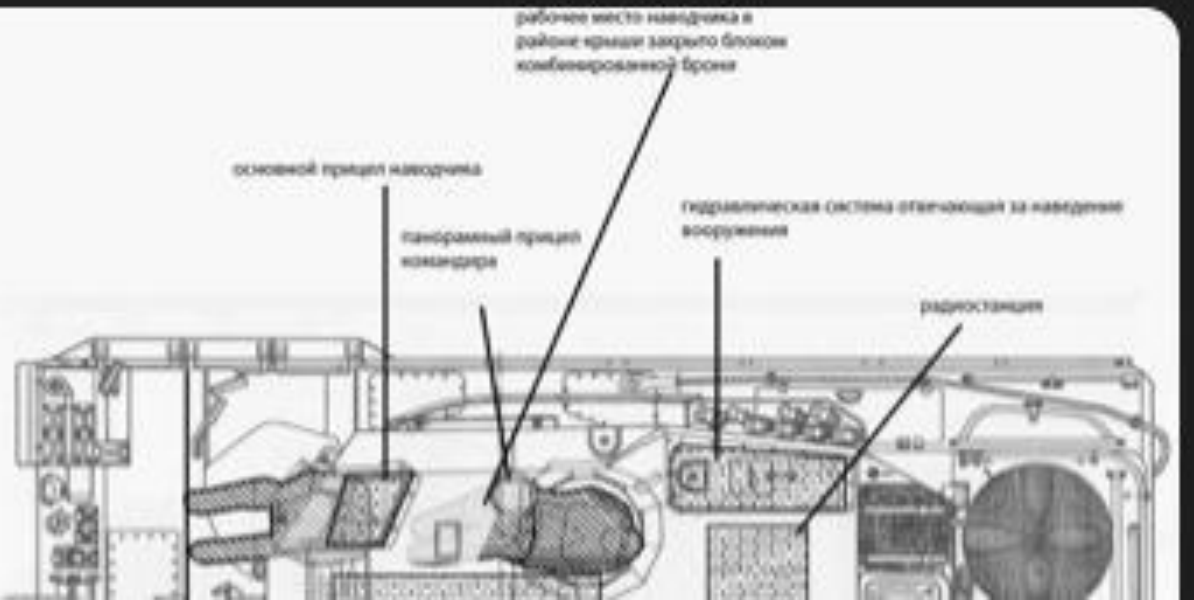
2.1.5.4 **Водитель**

2.1.5.2 **Наводчик**

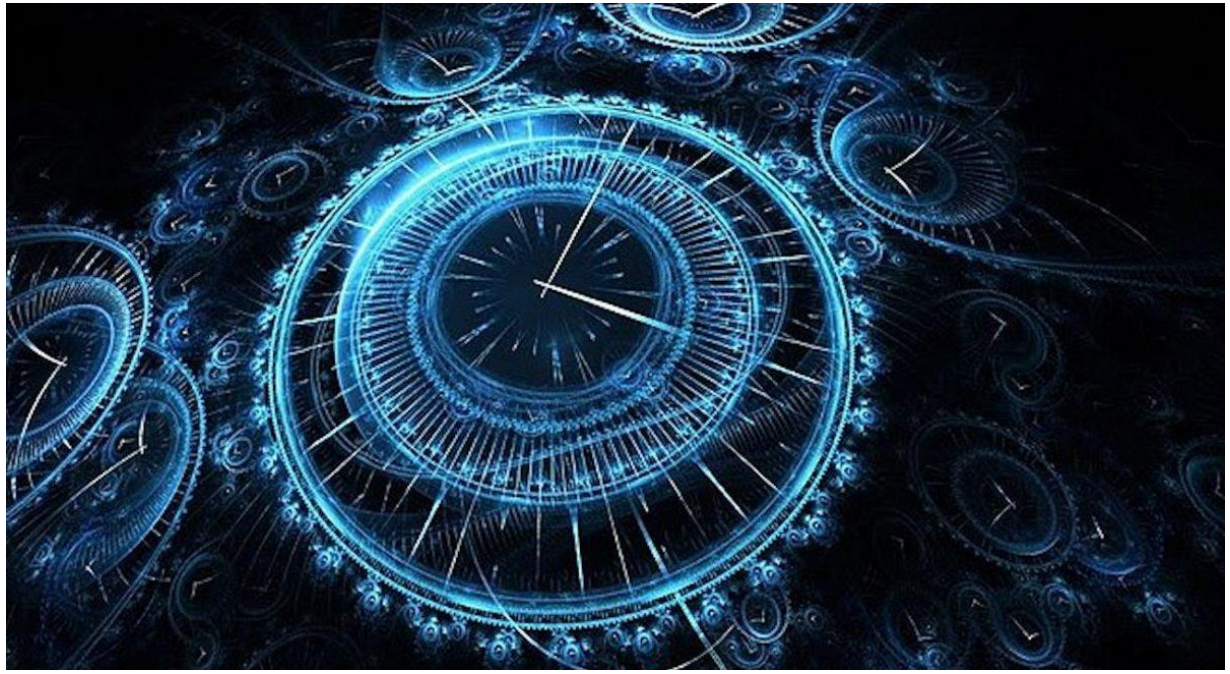


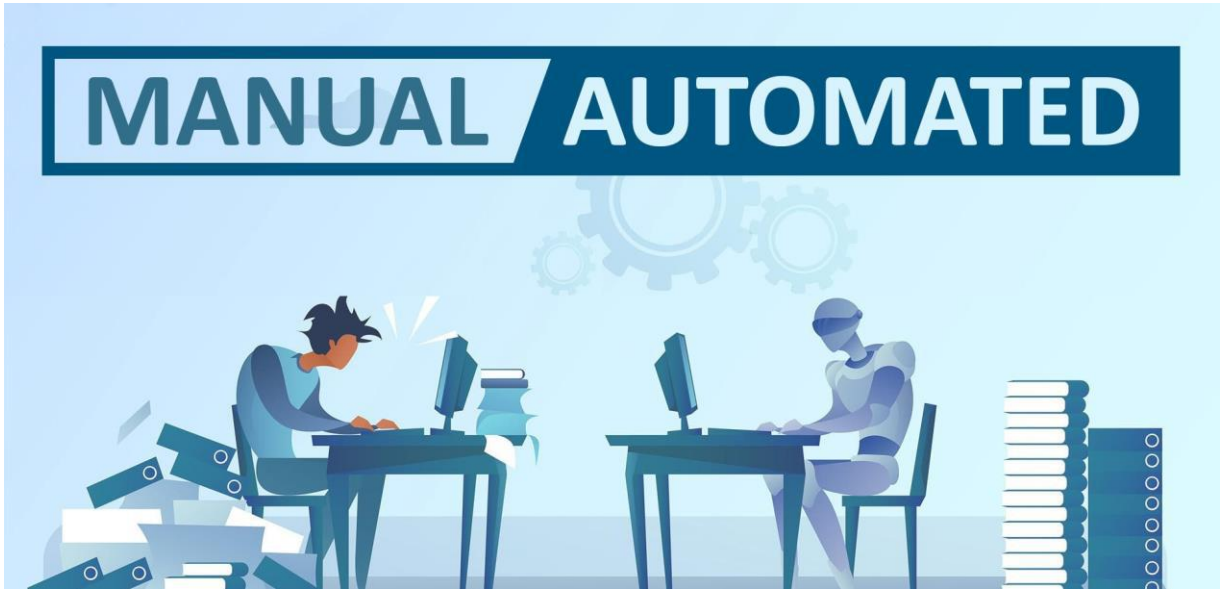
Непросматриваемое пространство с рабочих мест экипажа(заштрихованная область)

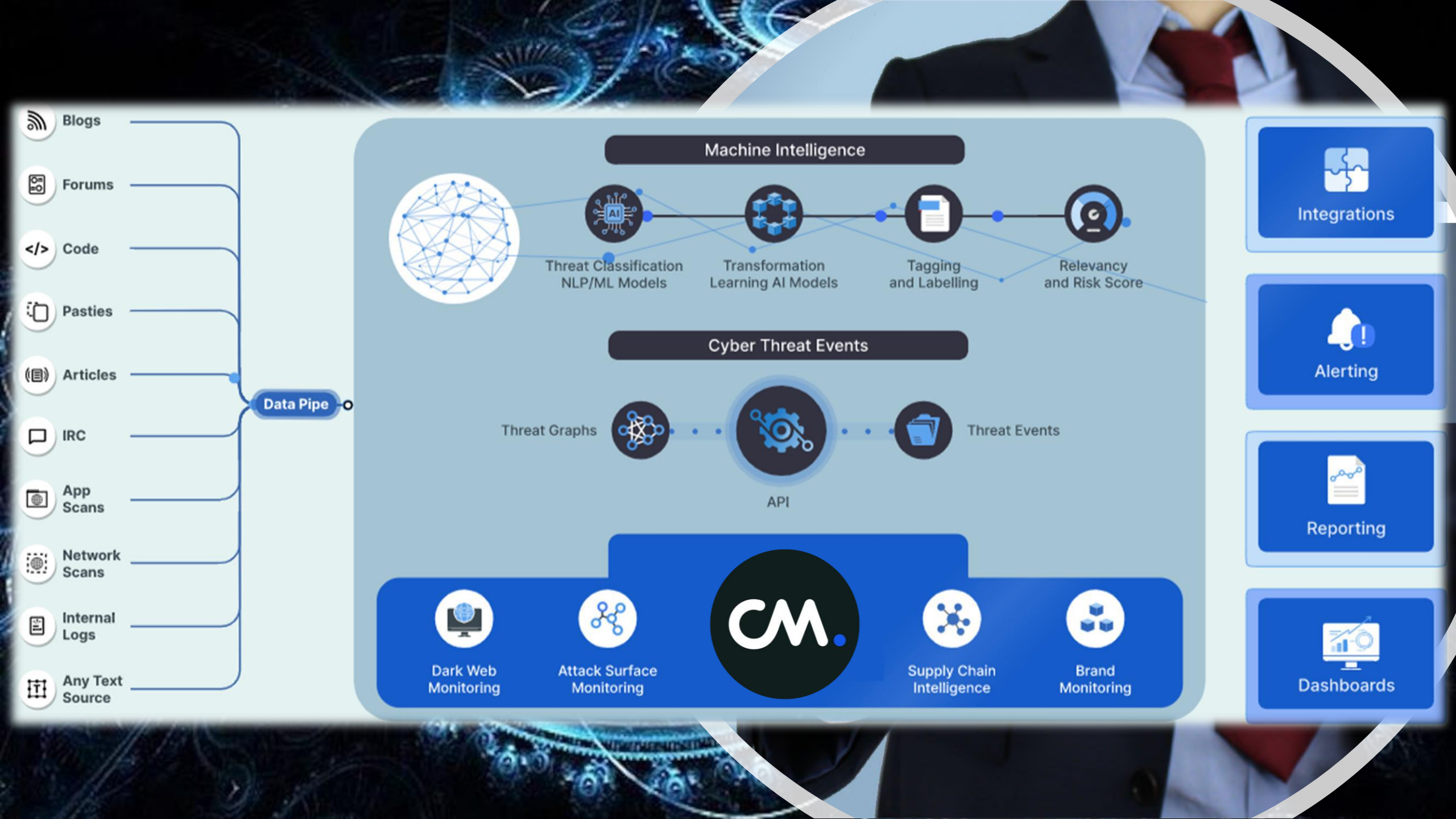




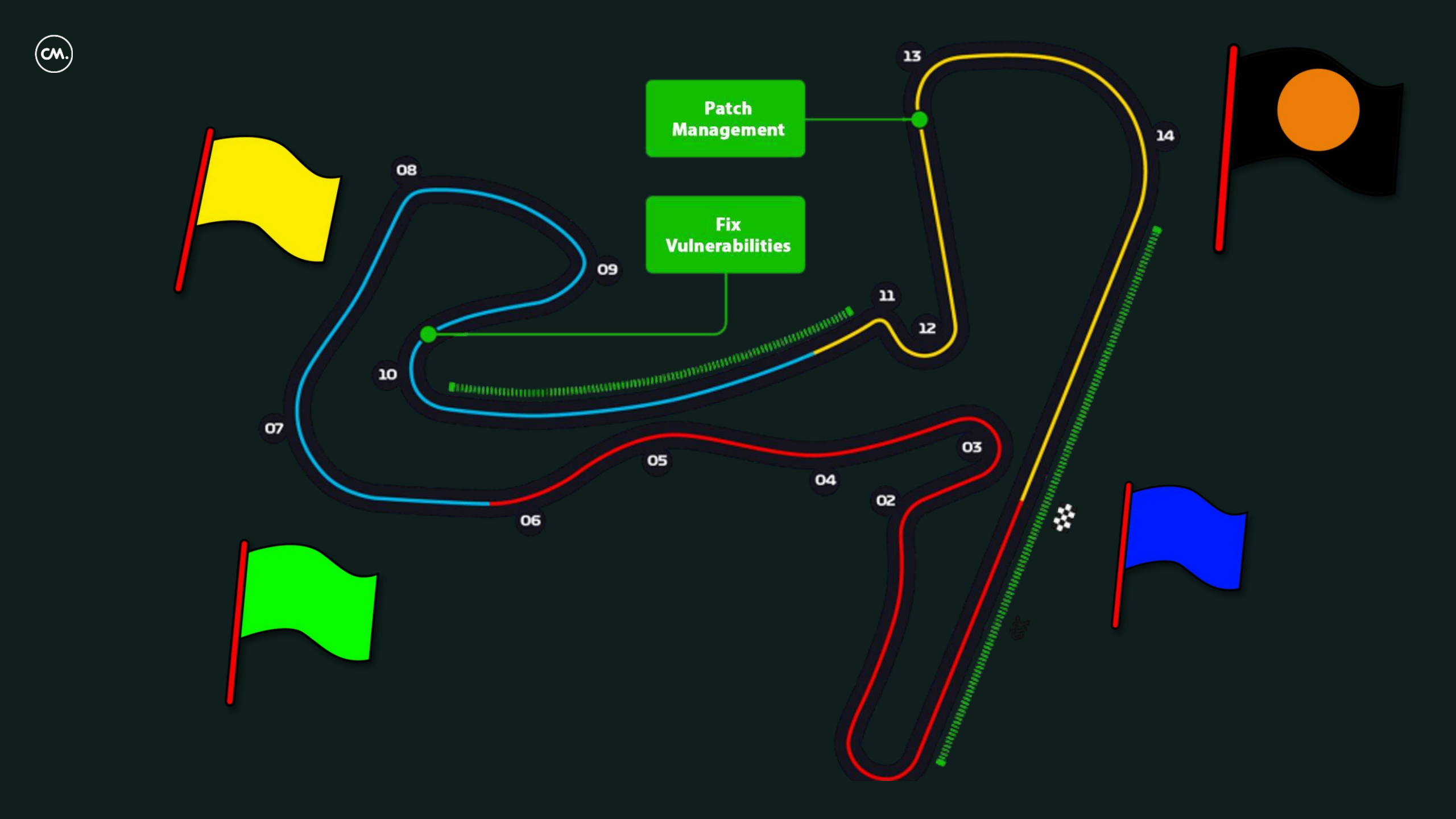

SMART




MANUAL
AUTOMATED


Blogs
Forums
Code
Pasties
Articles
IRC
App Scans
Network Scans
Internal Logs
Any Text Source
Data Pipe
Machine Intelligence
Threat Classification NLP/ML Models
Transformation Learning AI Models
Tagging and Labelling
Relevancy and Risk Score
Cyber Threat Events
Threat Graphs
Threat Events
API
Dark Web Monitoring
Attack Surface Monitoring
Supply Chain Intelligence
Brand Monitoring
Integrations
Alerting
Reporting
Dashboards

We Are Racing!


Patch Management
Fix Vulnerabilities
01
02
03
04
05
06
07
08
09
10
11
12
13
14


YOU HAVE BEEN
HACKED !

Thank you.